North Dakota Homeland Security Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners. If you have any comments to improve this summary or local information you would like to see in the summary please send the information to; kihagel@nd.gov

Quick Links

North Dakota

Storm caused $33 million in damage. North Dakota state officials have estimated that the April 2 snowstorm that has about 1,000 rural residents still living and working in the dark caused $33 million dollars worth of damage to the state's power infrastructure. The governor is seeking a federal disaster declaration for 12 North Dakota counties and the Standing Rock Sioux Indian Reservation. Heavy snow and strong winds that struck April 1 through April 3 crippled the electrical infrastructure in southwest and central North Dakota, toppling about 10,000 power poles and downing hundreds of miles of lines. As many as 8,400 people were without power after the storm. Source: http://www.kxnet.com/getArticle.asp?ArticleId=553898

REGIONAL

(Minnesota) **Minnesota communities to receive $12.3 million for water projects.** Six Minnesota communities, including Minneapolis, have received a total of $11.7 million in low-interest loans, and another got a $600,000 grant from the state for water-related, infrastructure improvements. Officials on Tuesday said that the total of $12.3 million from the Public Facilities Authority (PFA) is helping Minneapolis, South St. Paul, St. Bonifacius, Lowry, New Hope, East Bethel, and Chisholm. Lowry is the community that's getting the $600,000 grant from the PFA, which oversees financial management of three, revolving-loan funds and other programs that help Minnesota communities build facilities for clean water (including wastewater, stormwater and drinking water), as well as other kinds of public infrastructure projects. The PFA's three revolving funds are the Drinking Water Revolving Fund, the Clean Water Revolving Fund, and the Wastewater Infrastructure Fund. The authority is part of the Minnesota Department of Employment and Economic Development (DEED). Minneapolis got the biggest loan – $7.1 million at 1 percent interest over 12 years – to help pay for completing a project to upgrade an ultra-filtration plant. The favorable rate means that Minneapolis will save $734,790 when compared with market-rate financing, according to DEED. Along with the $600,000 grant from the PFA, Lowry also received a grant of $580,000 from the Small Cities Development Program, and a grant and loan of $2 million from the U.S. Department of Agriculture. Lowry will use all the money to pay for replacing the municipal wastewater collection system and building a wastewater treatment system. Lowry is in Pope County and has a population of 280. Source: http://www.finance-commerce.com/article.cfm/2010/04/14/123-million-going-to-Minnesota-communities-for-water-projects

(Minnesota) **Flood finally ebbing, Ft. Snelling park is reopening.** A sure sign that the flood season of 2010 has passed: Fort Snelling State Park in Minnesota has reopened. On Monday, the state department of natural resources announced the reopening of portions of the park, at the confluence of the Mississippi and Minnesota rivers. The park was closed on March 19 because of rising floodwaters. The department has reopened the main park road, the visitor center, memorial chapel and the Minnehaha and Snelling Lake trails. Still closed are Pike and Picnic islands, the Minnesota River boat landing and the Sibley trail. Source: http://www.startribune.com/local/90734489.html?elr=KArksLckD8EQDUoaEyqyP4O:DW3ckUiD3aPc:_Yyc:aUUZ

(Minnesota) **Suspicious note found on board Delta flight from Minneapolis to Atlanta.** TSA was made aware of a suspicious note that was found on a flight on the morning of April 9. The note was found in a seat pocket on board a Delta flight 1747 departing from Minneapolis-St. Paul International Airport that was heading to the Hartsfield-Jackson Atlanta International Airport. The flight landed without problem and the passengers that found the note were met by TSA and law enforcement and were questioned before being allowed to continue on their flight destinations. They authorities brought a canine unit to check for any problems and did not find anything. Source: http://www.digitalnewsreport.com/2010/04/09-suspicious-note-found-on-board-delta-flight-from-minneapolis-to-atlanta/3958

(Montana) **Brokerage fined $375,000 in data-breach case; alleged hackers arrested and extradited from Eastern Europe.** Anyone with a brokerage account with D.A. Davidson is likely to already have

heard about the breach in security and what the company has done to secure a remedy. As a penalty, the Financial Industry Regulatory Authority announced this morning that it has fined the Montana-based financial services firm $375,000 for failing to protect confidential, client information. The company's computer data were invaded, and confidential information downloaded, in 2008. The accused hackers, Latvian natives, then attempted to blackmail the firm. The company immediately reported the incident and assisted the Secret Service in identifying "four members of an international group suspected of participating in the hacking attack of the firm. Three of those individuals have been extradited from Eastern Europe, arrested and are facing charges in federal court in Montana," according to a FINRA release. To date, no clients have suffered any instance of identity theft related to the incident. Source: http://blog.thenewstribune.com/business/2010/04/12/brokerage-fined-375000-in-data-breach-case-alleged-hackers-arrested-and-extradited-from-eastern-europe/

National

Obama summit to highlight threat of nuclear terrorism. Nearly 50 countries are meeting in Washington this week for an unprecedented summit aimed at agreeing concrete action to prevent bomb-grade nuclear material from falling into the hands of terrorists. In a speech in Prague last year, the U.S. President warned that nuclear terrorism was the "most immediate and extreme threat to global security." He wants to use the summit to galvanize countries to take the issue more seriously. The goal of the summit is to reach a common understanding on the threat posed by nuclear terrorism and to agree on a plan of action to secure all loose nuclear material within four years to stop terrorists from getting their hands on it. The U.S. Secretary of State says the April 12-13 gathering of 47 nations is the largest conference hosted by the United States since 1945. Source: http://in.reuters.com/article/worldNews/idINIndia-47614020100412?pageNumber=2&virtualBrandChannel=0&sp=true

Higher hurricanes risk in 2010. Two months before the official start of the Atlantic hurricane season on June 1, Colorado State University researchers released their 2010 Atlantic hurricane season predictions based on 58 years of historical data, expecting it to be an above-average season due to the cooler ocean temperatures in the Pacific and warmer temperatures in the Atlantic. An average Atlantic hurricane season, which is officially from June 1 to November 30, has around 10 tropical storms, six of which have the chance to become hurricanes and 2 to become major hurricanes. But the predictions for this year show that 15 named storms might form in the Atlantic, eight of which may become hurricanes and four may be powerful hurricanes with winds of at least 111 mph. There is a 44 percent chance of a major hurricane making landfall on the East Coast, including Florida and the Gulf of Mexico oil patch, versus a long-term average of 30 percent, according to the researchers' predictions. Meanwhile, AccuWeather predicted a potentially "extreme" hurricane season for 2010, with 16 to 18 tropical storms almost all of them in the western Atlantic or the Gulf of Mexico, of which five hurricanes, two or three of them may be major and expected to hit the U.S. coast. However, it is the Colorado State University team predictions that are followed closely by the energy and commodity markets. Yet the team has repeatedly cautioned that the hurricane activity forecasts might be imprecise and can frequently miss predictions. Source: http://www.ecpulse.com/en/topstory/2010/04/08/2010-atlantic-hurricane-season/

INTERNATIONAL

Iceland's volcanic ash halts flights across Europe. An enormous ash cloud from a remote Icelandic volcano caused the biggest flight disruption Thursday since the September 11 attacks as it drifted over northern Europe and stranded travelers on six continents. Officials said it could take days for the skies to become safe again in one of aviation's most congested areas. The volcano beneath Iceland's Eyjafjallajokull glacier began erupting April 14 for the second time in less than a month. The cloud, floating miles above Earth and capable of knocking out jet engines, wrecked travel plans for tens of thousands of people. All non-emergency flights in Britain were canceled until at least midday April 16, and authorities in Ireland, Denmark, Norway, Sweden, Finland, and Belgium also closed their air space. France shut down 24 airports. In Germany, airports in Berlin and Hamburg were shut the evening of April 15. Several U.S. flights bound for Heathrow, including those from Chicago, San Francisco, Denver, Las Vegas and New York, had to return to their departure cities or land elsewhere when London airports were closed. In Washington, the Federal Aviation Administration said it was working with airlines to try to reroute some flights around the huge ash cloud, which is hundreds of miles wide. The Icelandic plume lies above the Atlantic Ocean close to the flight paths for most routes from the U.S. East Coast to Europe, and was moving over Europe itself. Meteorologists from the AccuWeather forecasting service in Pennsylvania said the current ash plume will threaten air travel over Europe through April 18 at the least. A geophysicist at the Icelandic Meteorological Office said the problem might persist for weeks, depending on how much wind carries the ash. Source: http://www.google.com/hostednews/ap/article/ALeqM5jh7lQ-qBxQMPzPd3Iap7_s3YDBfQD9F3MO900

Strong quake kills hundreds in western China. A powerful earthquake in western China killed at least 400 people, injured 10,000 and left many others buried under debris on Wednesday, Chinese state media reported. The quake, which struck at 7:49 a.m. in Qinghai Province, bordering Tibet, had a magnitude of 7.1, according to China's earthquake agency. Workers were rushing to release water from a reservoir after cracks were discovered in a dam, according to the China Earthquake Administration. The China Earthquake Networks Administration said the quake struck in Yushu County, a remote and mountainous area sparsely populated by farmers and herdsmen. Source: http://www.nytimes.com/2010/04/15/world/asia/15quake.html

Islamic militant attacks leave 15 dead in Philippines. Al Qaeda-linked militants in police uniforms set off bombs and fired at civilians on a strife-torn Philippine island Tuesday in violence that left 15 people dead, officials said. The gunmen detonated two home-made bombs near a church and a school sports grandstand in Isabela city on Basilan island, in the latest show of force by the Abu Sayyaf network, which is blamed for the nation's worst terrorist attacks. "I think (the attack) is meant to create havoc.... Definitely it falls under terrorism," the head of the Philippine Marines told reporters in Manila. Isabela's mayor told reporters that 15 people were confirmed dead, including five militants who were apparently killed by one of their own bomb blasts. Six civilians were also killed in the explosions, while three soldiers and a policeman were killed in gun battles with the militants, the Marine leader said. At least 25 militants wearing police uniforms were involved in the attacks, according to the region's military chief. However he said the Abu Sayyaf's main goal may have actually been to kidnap a high-profile person in Isabela, and that the explosions could have been intended as a diversion. "It looks like they were planning to kidnap someone but they did not expect

our troops to react immediately," the military chief said, adding he did not know the target of the suspected abduction plot. The militants sprayed bullets at terrified civilians scrambling for safety, and engaged in a gun battle with security forces on the outskirts of Isabela that lasted for at least three hours, according to military chiefs. Source: http://www.google.com/hostednews/afp/article/ALeqM5gntsuwZXYtcUV8WPVp-2WdVnWY_w

WHO admits shortcomings in handling flu pandemic. The World Health Organization on Monday conceded shortcomings in its handling of the H1N1 swine flu pandemic, including a failure to communicate uncertainties about the new virus as it swept around the globe. The WHO's top influenza expert said the U.N. agency's six-phase system for declaring a pandemic had sown confusion about the flu bug which was ultimately not as deadly as the widely-feared avian influenza. "The reality is there is a huge amount of uncertainty (in a pandemic). I think we did not convey the uncertainty. That was interpreted by many as a non-transparent process," he said. He was addressing a three-day meeting of 29 external flu experts called to review WHO's handling of the first influenza pandemic in 40 years. Critics have said the WHO created panic about the swine flu virus, which turned out to be moderate in its effect, and caused governments to stockpile vaccines which went unused. Source: http://www.reuters.com/article/idUSTRE63B2TL20100412

Russia points to human error in fatal Polish crash. Russian investigators suggested human error may have been to blame in the plane crash that killed the Polish president and 95 others, saying Monday that were no technical problems with the Soviet-made plane. The Polish government-owned Tu-154 went down while trying to land Saturday in dense fog near Smolensk airport in western Russia. The pilot had been warned of bad weather in Smolensk, and was advised by traffic controllers to land elsewhere. Polish investigators have not yet listened to the cockpit conversations recorded on the black boxes, but will, to see if there were "any suggestions made to the pilots" from other people aboard the plane to land at Smolensk instead of diverting to Minsk or Moscow. Source: http://www.google.com/hostednews/ap/article/ALeqM5h5HRIwocn5cLZn75suY8xsI5-1bgD9F1HVDO1

Landslide derails train in northern Italy, 9 dead. A cascade of rocks and debris slammed onto a small commuter train traveling through the Italian Alps in northern Italy near the Austrian border, causing it to derail and killing at least nine people while injuring another 30 aboard. One of the two train cars was destroyed, its windows shattered, ANSA news agency reported, adding that about 40 people had been on board at the time of the accident. "The landslide occurred at the very passage of the train," said a transport official in nearby Bolzano city. He said the burst pipe had triggered the rock fall onto the train around 9:30 a.m. Temperatures were too high to freeze the water in the pipe; authorities said they were investigating why it had burst. Source: http://www.businessweek.com/ap/financialnews/D9F1JLG80.htm

Violence impacts Reynosa maquilas; gunmen attack oil firm. Gunmen charged after midnight April 9, making off with uniforms and at least five trucks from the world's largest oilfield services company. It is unclear if the attackers were from a drug cartel or how they even managed to bypass the security gate and guards at the Schlumberger Ltd. compound on the western outskirts of Reynosa, Mexico. Cartels have commandeered cargo trucks loaded with goods and buses for factory workers to create impromptu roadblocks. Factories have canceled shifts on violent nights when they felt it was too unsafe for workers to leave home or when they could not catch the bus. "We're at a tipping point. If

something is not done, there's going to be an impact to this (industry)," one factory manager said. None of the 140 maquiladoras in Reynosa's 11 industrial parks are pulling out of the area, managers said, but many have developed exit strategies in case the violence does not abate. For now, the majority of the manufacturers have barred non-essential travel to Mexico, and many of those factories' vendors and suppliers now refuse to cross the border, according to managers and industry insiders. "In the short term, they're taking a wait-and-see approach," said the president and CEO of the McAllen Economic Development Corp., an organization that has aggressively recruited manufacturers to Reynosa for more than two decades. Manufacturers such as LG Electronics, Black & Decker, Motorola, and Nokia employ more than 72,000 in Reynosa. Source: http://www.themonitor.com/articles/violence-37338-factories-fear.html

Banking and Finance Industry

FDIC plans $1.97 billion sale of loans from 22 seized banks. The Federal Deposit Insurance Corp. (FDIC) is seeking bids on a $1.97 billion portfolio of loans from 22 seized banks, pushing the agency's structured asset sales this year beyond the 2009 total. The sale consists of 1,739 loans mostly tied to commercial real estate, with borrowers late on payments for almost half the portfolio, according to a preliminary announcement obtained by Bloomberg News. Barclays Capital was listed as the marketing agent for the sealed-bid auction. The FDIC is stepping up sales of assets accumulated by the bank regulator as 182 firms have failed since January 2009. The agency is trying to restore its deposit insurance fund, which posted a $20.9- billion deficit last year after lenders collapsed at the fastest pace in two decades. The new portfolio will be sold as a structured transaction, which means the FDIC will share ownership and proceeds with the winning bidder, the announcement said. The FDIC may contribute financing, the announcement said. Source: http://www.bloomberg.com/apps/news?pid=20601103&sid=athIqKK8SwpM

(Arizona) **Police: Bank robber threatened tellers with explosives.** A 72-year-old man has been arrested after police say he robbed a Compass Bank located inside an Albertson's supermarket in Prescott, Arizona. Prescott Police said that the suspect entered the bank, showed tellers a handgun and claimed he had put explosives in the store on April 8. He robbed two tellers of an undisclosed amount of cash, as well as some personal money, according to police. The suspect was taken into custody immediately after he exited the bank. The store was evacuated and searched for explosives but nothing was found. Source: http://www.myfoxphoenix.com/dpp/news/crime/bank-robber-explosives-4-8-2010

(California) **Ex-employees turn to cyber crime after layoffs.** When a slumping economy and historically high unemployment rates dropped the ax on the country's workforce and left the survivors wondering if — or when — they'd be next, law enforcers and security experts braced themselves for what they considered would be an almost inevitable rise in data breaches and high-tech crimes. Based on new data, it appears they may have been right. National unemployment rates peaked in October at 10.1 percent and remained at 9.7 percent during the first two months of the year. Local law enforcement officials said the inability to find gainful employment has been a recurrent motivation behind new cases of identity theft and software piracy that drop on their desks almost daily. In one recent case under investigation, a detective sergeant said, an unemployed San Mateo, California woman in her 20s was detained with a large number of re-encoded credit cards in her possession. She said she was using them to buy food. And a Fremont, California man who had

been recently laid off was arrested in February for selling pirated copies of a $2,500 Adobe design program for $150 on Craigslist. According to cybersecurity researchers, corporations across all industries have been dealing with a steadily growing number of internal data breaches since the financial meltdown. Source: http://seattletimes.nwsource.com/html/nationworld/2011588615_cybercrime14.html

Chemical and Hazardous Materials Sector

(Florida) **Suspicious container found outside building.** Miami Fire Rescue Haz Mat units and a bomb squad are investigating a suspicious container that was left outside of a South Florida building. The incident occurred Thursday around 7 a.m. near 13th Terrace and Northwest 14th Avenue after reports came in regarding a radiological container found in the area. Traffic in the area will remain blocked off until the investigation is complete. Source: http://www.wsvn.com/news/articles/local/MI84525/

7 in hospital after radiation exposure in India. Seven people have been admitted to a New Delhi hospital after being exposed to radioactive waste, police said Wednesday, raising fears over the lax disposal of hazardous material in India. Radioactive waste was detected in a congested, scrap-metal market last week when five people were rushed to a hospital after they showed symptoms of radiation exposure. Two more victims have since been admitted. “Seven people have been hospitalized and we are yet to find the exact source of the radioactive leakage,” a senior police officer told AFP on Wednesday. “No one has been detained or arrested as of now.” Reports of the incident triggered panic in residential areas surrounding the scrapyard in western New Delhi, which deals with metal and old ammunition. Police said they had found the carcinogen cobalt-60 at the site, a radioactive metal used for radiotherapy in hospitals and sterilization in industrial-food processes. The U.S. Environmental Protection Agency’s Web site warns that cobalt-60 can make its way into landfill and scrap-metal yards undetected because it is often encased in a metal housing. A team of scientists from the Bhaba Atomic Research Centre, India’s leading atomic research institute, have cordoned off the affected area. One expert said the incident highlights the country’s poor enforcement of rules on radioactive waste disposal. Source: http://www.google.com/hostednews/afp/article/ALeqM5j-Mys338qJYOQxgdE2ZLsl3drSvQ

Commercial Facilities

DHS program develops mass evacuation simulation for stadiums. Sports venues are supposed to be prepared for emergencies — such as a bombing or a lone shooter — that could require a quick evacuation of more than 70,000 fans. But venue managers “are not training their staffers as well as we would like,” said the director of the National Center for Spectator Sports Safety and Security (NCSSSS). “They’re not doing training exercises,” he said, noting that it’s costly to conduct live drills for events of this magnitude. The NCSSSS director is one of the leading researchers in a project that seeks to fill these training deficiencies. The Department of Homeland Security’s science and technology directorate partnered with the University of Southern Mississippi and several other organizations to create a computer program called SportEvac that uses human avatars to simulate the behaviors of panicking crowds in sports stadiums. “Our goal was to try to find ways to reach security planners and give them a tool suite they can use for practicing these scenarios,” said the

NCSSSS director. The program can be customized to fit the specifications of individual stadiums. It uses algorithms to predict the behaviors of large groups, and it factors in variables such as irrational, drunken fans and wheelchair-bound spectators. Managers can determine how long an evacuation would take, how many people would crowd each exit and where signs could be placed to improve efficiency. The underlying concepts can be applied to evacuation simulations for shopping malls, concert halls and other crowded events, the NCSSS director said. "This is just the beginning of the capabilities," he added. "I hope that this modeling is carried over to other areas of critical infrastructure as a gift from the sports world." In March, developers began testing the software by applying its models to actual stadiums. They're also looking into options for commercializing the software, which they hope to get into the hands of as many stadium managers as possible. DHS spent $1.3 million on the project. Source: http://www.nationaldefensemagazine.org/archive/2010/May/Pages/MassEvacuationSimulationforStadiums.aspx

(Missouri) **Suspicious backpack destroyed outside insurance office in Springfield.** The Springfield (Missouri) Bomb squad destroyed a suspicious backpack early this morning found outside PJC Insurance on Norton Road. The assistant fire chief said the backpack was found in the middle of the parking lot before 7 a.m. It was leaking some type of acid that was eating through the asphalt of the lot. After evacuating personnel at the insurance firm and closing the south side of nearby Lowe's, the bomb team dug a hole and destroyed the bag. "It was just a lot safer to get rid of it," the assistant fire chief said. He said they do not know what was inside the bag, but it's placement in the lot, away from the building and cars, seemed to indicate that it wasn't meant to be explosive. Source: http://www.news-leader.com/article/20100413/BREAKING01/100413031/1007/NEWS01/Suspicious+backpack+destroyed+outside+insurance+office+in+Springfield

(Indiana) **Suspicious powder in mail leads to closing of Academy of Model Aeronautics.** The Academy of Model Aeronautics in Muncie voluntarily closed its headquarters and museum on Friday after a mail clerk opened a suspicious envelope that arrived in the mail. The envelope contained a white powder and nothing else. "The consensus was that this was pretty much a hoax, but in this day and age, until we find out what it turns out to be, we erred on the side of caution," said the executive director of AMA, which employs 55 people. The staff was sent home for the day and a sign on the front door said the building would remain closed until further notice. County police took possession of the envelope from AMA. Police did not return several calls from the Star Press on Friday regarding whether they had identified the substance. Police arrived at AMA around 8:30 a.m. and left 45 minutes later. No emergency management agency, hazardous material, fire or emergency medical services personnel were called to the scene — indicating it is unlikely they believe anthrax is involved. "We followed protocol and contacted the state's homeland security," said the director of the local emergency management agency. "The sheriff is investigating the envelope and has possession. They are holding it to see if they need outside resources (to identify it)." There is no report of any illness. Source: http://www.thestarpress.com/article/20100410/NEWS01/4100309/1002

(Oklahoma) **Muskogee mall to reopen after deadly weekend shooting.** Arrowhead Mall in Muskogee will be back open Monday following a deadly shooting over the weekend. One person was killed and five others were injured. So far, three of the victims that were injured have been released from the hospital, and this morning police are still searching for "three" suspects. Officers have made

no arrests in this case, but they do have a good idea of whom they are looking for. In what may have been a gang shooting, police say they know there were at least two intended targets, and four innocent bystanders who got caught in the line of fire. The Muskogee Police Department is asking for help from the public this morning on any leads they might have. Police are looking for a 20 year old suspect. Officers say he does have a prior criminal record. Police are also searching for two juveniles, a 16 year old and a 17 year old. Source: http://www.fox23.com/news/local/story/Muskogee-Mall-To-Reopen-After-Deadly-Weekend/yK_oSmbUQka7_ELeVKjZ1Q.cspx

Communications Sector

European Union, France to consult on net neutrality. The European Commission will launch a public consultation on the issue of network neutrality this quarter, the commissioner for the digital agenda said on April 13. She intends to report back to the European Parliament before the end of the year on whether regulatory action on net neutrality is necessary. However, she set the bar for introducing new regulation high, stating it must be justified by the need to tackle specific problems. The debate over net neutrality is already under way, and not just in the U.S., where the question of whether the U.S. Federal Communications Commission can mandate it has already reached the courts. The recently created Body of European Regulators for Electronic Communications (BEREC), which brings together the national regulatory authorities of E.U. member states, has already set up a project team to work on net neutrality issues, the commissioner said. One of the most important factors for all concerned parties is what they mean by net neutrality. Source: http://www.computerworld.com/s/article/9175424/European_Union_France_to_consult_on_net_neutrality

A Chinese ISP momentarily hijacks the Internet. For the second time in two weeks, bad networking information spreading from China has disrupted the Internet. On April 8, bad routing data from a small Chinese ISP called IDC China Telecommunication was re-transmitted by China's state-owned China Telecommunications, and then spread around the Internet, affecting Internet service providers such as AT&T, Level3, Deutsche Telekom, Qwest Communications, and Telefonica. "There are a large number of ISPs who accepted these routes all over the world," said the technical lead at Internet monitoring firm Renesys. The incident started just before 10 a.m. Eastern Time on April 8 and lasted about 20 minutes. During that time IDC China Telecommunication transmitted bad routing information for between 32,000 and 37,000 networks, redirecting them to IDC China Telecommunication instead of their rightful owners. These networks included about 8,000 U.S. networks including those operated by Dell, CNN, Starbucks, and Apple. More than 8,500 Chinese networks,1,100 in Australia and 230 owned by France Telecom were also affected. The bad routes may have simply caused all Internet traffic to these networks to not get through, or they could have been used to redirect traffic to malicious computers in China. While the incident appears to have been an accident, it underscores the weakness of the Border Gateway Protocol. Source: http://www.pcworld.com/article/193849/a_chinese_isp_momentarily_hijacks_the_internet.html

(Virginia) **Verizon kicks off disaster recovery drill.** Hundreds of Verizon Communications Inc. employees are involved in this week's disaster recovery exercise, which is the first that encompasses all of Verizon Telecom and Verizon Wireless operations. The week-long event begins April 12 with a simulated disaster involving a mid-air collision that sends a commercial airliner crashing into a major Verizon facility at its Ashburn, Virginia corporate campus, and also causes damage to a Leesburg,

Virginia local phone company Central Office. It continues April 13 with simulated chlorine leak from a tanker truck that compromises a major data center at Ashburn as well, and requires Verizon's hazardous materials team to respond. Later in the week, the FBI will be on hand to discuss terrorism and other network threats. The idea is to have each unit of Verizon put its disaster recovery plan into place and then evaluate how the plan actually works and where changes/improvements might be needed. On display in Virginia will be Verizon's latest addition to its disaster recovery fleet, a 51-foot Mobile Command Center, as well as housing trailers, comfort trailers, satellite trailers, hazmat vehicles, and more, all designed to enable Verizon to independently operate following any kind of disaster. Source:
http://www.lightreading.com/document.asp?doc_id=190330&f_src=lightreading_gnews

Windows Mobile trojan makes long distance calls. Some Windows Mobile phones owners are reporting online that their cellphones have been making expensive calls to a variety of destinations without their permission. Security researches from Sophos observe that a trojan named Troj/Terdial-A is the malicious program that is making unauthorized phone calls from users' phones. All of the affected phone owners have downloaded and installed a 3D action game on their cellphones. It became clear that a Russian-speaking hacker has infected versions of a 3D anti-terrorist action game with malicious trojan program hidden inside. The trojanized version of the game is uploaded to several Windows Mobile freeware download sites. Windows Mobile phone users are warned to beware of downloading games to their devices from freeware and warez sites. Source:
http://www.pc1news.com/news/1279/windows-mobile-trojan-making-long-distance-calls.html

Defense Industrial Base Sector

US military testing high-tech dirigibles in Utah; 'aerostats' meant to detect cruise missiles. The skies over the Utah desert are becoming the test site for a new fleet of hulking, high-tech dirigibles the U.S. military hopes will provide battlefield commanders a bird's-eye view of cruise missiles and other threats. One of the unmanned balloons — a 242-foot-long craft known as an aerostat — was launched Wednesday morning about 80 miles west of Salt Lake City. It stayed aloft for about three hours before it was pulled back down. It was the first of several tests expected in the coming year or so in Utah, according to a spokeswoman for Dugway Proving Ground. Vast tracts of military-owned desert were chosen for the testing because of their remote location and resemblance to the mountainous, arid environment of Afghanistan, the military said in a statement. The dirigibles are outfitted with radar and communications systems to provide long-range, surveillance targeting threats from aircraft, ballistic and cruise missiles. Military officials said the aerostats will be less expensive to maintain and operate than conventional aircraft-based radar while providing battlefield commanders a bird's-eye view of threats in a given area. Source:
http://www.latimes.com/news/nationworld/nation/wire/sns-ap-us-military-tests-dirigibles,0,5339880.story

Former B-2 engineer accused of spying for China. Federal prosecutors on Tuesday accused a former B-2 stealth bomber engineer of betraying the U.S. by selling military secrets to China, but his defense countered that the information he passed on was "obvious" and "well-known." The man, 66, disclosed "vulnerabilities of our nation's most important strategic assets" and helped design a stealth cruise missile for China that would evade infrared sensors and defeat U.S. heat-seeking missiles, an assistant U.S. attorney told jurors during opening statements. The India-born naturalized U.S. citizen

did so — and also marketed his services to Switzerland, Israel and Germany — in part because he desperately needed more money to pay the mortgage on his mansion-like home overlooking Maui's North Shore, the prosecutor said. The engineer has pleaded not guilty to 17 counts, including conspiracy, violating the arms export control act and money laundering. He has been held in federal detention since his October 2005 arrest because a judge decided he was a flight risk. His defense attorney told jurors that the information his client passed to others wasn't classified. He argued that the cruise-missile, exhaust-nozzle design that the engineer sold to China used obvious, well-known information. Source:
http://www.militarytimes.com/news/2010/04/ap_airforce_espionage_china_041410/

Corps makes progress on LAV upgrades. The Corps is on the verge of completing significant upgrades to the Light Armored Vehicle, with new armor, safer crew cabins and better seats in planning and development this year. The LAV-25, comprising 400 of the Corps' 870-plus LAV fleet, will receive new fuel tanks placed farther away from the Marines inside. The vehicle, carrying two crewmen and six combat-ready Marines, currently places Marine scouts in an observation post directly on the fuel cell, raising safety concerns. Marine officials did not say where the new tank will be located, but the Corps has tested several prototypes and plans to open a contract competition this year, said a spokesman for Marine Corps Systems Command. The Corps also is working to replace bench seating with new blast-resistant seats. Several options have been blast tested, and the service also developed a crew compartment layout necessary to fit the seats. Marine officials did not describe the revised layout, but said it is undergoing user evaluations, and could be finalized if Marines testing it view it favorably. Additionally, the service is testing new, lighter underbelly armor that would increase the vehicle's mobility when up-armored. Testing should be completed this year, allowing the Corps to integrate changes onto existing vehicles. Source:
http://www.militarytimes.com/news/2010/04/marine_lav_040910w/

Army impressed by initial test of next generation radios. Army officials said last Thursday they have been impressed by early tests at this sprawling 3,200-square-mile base of an advanced radio that is designed to send huge files of maps and images to soldiers in the field and improve transmissions in mountainous areas such as Afghanistan. The next generation devices, called ground mobile radios, are wideband versions of the Joint Tactical Radio System under development since 1996 and have sent data as far as 19.5 miles during tests this week, said the program manager for the Army's infantry brigade combat team integration project. The radios are a central part of the Army's plan to modernize its brigades and will link units so that they can communicate not only by voice but transmit broadband data, including imagery. The Army plans to continue testing the new radios, developed by Boeing, through June and expects its range to increase. In addition, the latest version exceeded its required throughput of 2 megabytes per second, a generational leap from existing radios, said a product manager for the ground mobile radio at the JTRS program office in San Diego. He attributed the increased performance to improvements in the software, which was not fully developed when the radios were tested in 2009. In March the Defense Department's director of operational test and evaluation, told lawmakers at a House Armed Services Committee hearing that the radios had suffered a slip in development testing last year because of hardware and software problems, which resulted in low throughput. JTRS has been in development since 1996. This year the tests involve units across more than 350 square miles, similar to a setting in which the 1st Armored Division's 3rd Infantry Brigade Combat Team will operate when it is deployed to Afghanistan, said the director of operations for the integration project. The terrain and scenarios will mimic operations in

Afghanistan, including mountainous areas that can block radio signals and in villages. Source: http://www.nextgov.com/nextgov/ng_20100409_1179.php

CRITICAL MANUFACTURING

Toyota suspends sales of Lexus GX 460. Toyota asked dealers to temporarily suspend sales of the new 2010 Lexus GX 460 after Consumer Reports issued a safety warning on the SUV. "We are taking the situation with the GX 460 very seriously and are determined to identify and correct the issue Consumer Reports (CR) identified," the Lexus Group vice president and general manager, said in a prepared statement. Earlier on Tuesday, CR said there was an increased risk of rollover during a turn, a problem it uncovered during routine tests. It urged car shoppers not to buy the GX 460 until the problem is remedied. The special designation given to the GX 460 by Consumer Reports — "Don't Buy: Safety Risk" — is rarely given by the magazine. The last time it was used was in 2001, on the Mitsubishi Montero Limited. About 5,000 GX 460s have been sold in the roughly three months the model has been on sale, the magazine said. It advises current owners of this vehicle to approach exit ramps with caution, and to call Toyota demanding a fix for the problem. Toyota said earlier that the GX 460 "meets or exceeds all federal government testing requirements." The SUV's electronic stability control (ESC) program failed to keep the vehicle in line during a severe-handling maneuver, allowing it to slide almost completely sideways, said a CR spokesman. He said that situation could lead to a rollover. ESC is a computerized system that controls the brakes and accelerator to help maintain vehicle control in abrupt maneuvers. The problem with the Lexus' ESC system became apparent during tests designed to detect a specific, emergency-handling problem — one in which a vehicle's back end slides outward when the driver lifts his foot from the gas pedal during a turn. The GX's ESC system did not become active until the SUV had already skidded dangerously, the CR spokesman said. "We're in the process of testing the 2010 Lexus GX 460 SUV to ensure it complies with NHTSA's safety standard for electronic stability control ESC, and to understand better the results obtained by Consumers Union reported today," a spokeswoman for the National Highway Traffic Safety Administration said in a statement. "It is our belief that ESC should prevent the kind of fishtail event described." Source:
http://money.cnn.com/2010/04/13/autos/consumer_reports_lexus_gx460/

Toyota could face a second U.S. fine. The National Highway Transport Safety Administration could slap another fine on Toyota after the $16.4 million penalty it imposed for the Japanese carmaker's not disclosing facts faster on involuntary acceleration. The first fine was imposed after a Department of Transportation review of 70,000 pages of documents found Toyota "knowingly hid a dangerous defect for months from U.S. officials and did not take action to protect millions of drivers and their families." And in a letter to Toyota obtained on April 10 by Agence France Presse, the NHTSA warned Toyota it was considering a second penalty. Toyota recalled more than nine million vehicles worldwide including more than six million in the United States mainly for involuntary acceleration problems but also for some faulty brakes on some hybrid vehicles. Problems related to sudden, unintended acceleration that have been blamed for more than 50 U.S. deaths and resulted in the recall of more than eight million vehicles worldwide. Toyota is facing at least 97 lawsuits seeking damages for injury or death linked to sudden acceleration and 138 class action lawsuits from angry customers suing to recoup losses in the resale value of Toyota vehicles following the recalls. Source:
http://www.industryweek.com/articles/toyota_could_face_a_second_u-s-_fine_21557.aspx

Emergency Services

(New Jersey) **Camden man arrested for shining laser pointer at helicopter.** New Jersey Air National Guard helicopter pilots have helped Camden police with day and nighttime patrols for the last eight months or so on a "routine basis," the police chief said Tuesday night. His comments came after Camden police announced that a 32-year-old man was arrested and charged with flashing a laser pointer at a National Guard helicopter patrolling with police last week, officials said. He was charged with interference with transportation, a Camden police spokeswoman said. The suspect was released with a summons. He allegedly pointed a green laser at the helicopter on April 8, temporarily blinding the pilot. Police on the ground located him at Alabama and Congress Roads, sitting inside a red, Dodge minivan. He allegedly told police he thought he was pointing the laser at a news helicopter. The pointer was found in the minivan's glove compartment. Source: http://www.philly.com/philly/business/technology/20100414_Camden_man_arrested_for_shining_laser_pointer_at_helicopter.html

Feds say Border Patrol vehicles being 'cloned' by Mexican smugglers. Federal agents along the Texas border were warned by the Department of Homeland Security that Mexican drug cartels are using "cloned" Border Patrol vehicles to smuggle drugs into the United States, according to documents obtain by the Washington Examiner. The DHS report was sent to Border Patrol officials in Webb County, Texas, in March. It asked Border Patrol agents and local law enforcement officials to be on alert for "a suspected cloned marked Crown Victoria" the same vehicle type used by the agents. The alert was part of a "significant incident report," which contains information that is not to be made public or released to the media. A U.S. law enforcement Official, with knowledge of drug cartel operations along the border, said "cloned vehicles pose a significant problem for both law enforcement and citizens." He said, "It's especially dangerous since attacks against federal and local law enforcement agents has increased over the past year. The cartels are finding more innovative ways to move across the border and we have to be one step ahead of them." The danger has increased for federal agents on the border, figures showed. Source: http://www.washingtonexaminer.com/world/Feds-say-Border-Patrol-vehicles-being-_cloned_-by-Mexican-smugglers-90405964.html

Energy

US military warns oil output may dip causing massive shortages by 2015. In a new Joint Operating Environment report from the U.S. Joint Forces Command, the U.S. military has warned that surplus oil-production capacity could disappear within two years and there could be serious shortages by 2015. Such a situation would have significant economic and political impacts, the study indicated. "By 2012, surplus oil-production capacity could entirely disappear, and as early as 2015, the shortfall in output could reach nearly 10 million barrels per day," the report stated. "While it is difficult to predict precisely what economic, political, and strategic effects such a shortfall might produce, it surely would reduce the prospects for growth in both the developing and developed worlds," the study continued. "Such an economic slowdown would exacerbate other unresolved tensions, push fragile and failing states further down the path toward collapse, and perhaps have serious economic impact on both China and India." The U.S. military said its views cannot be taken as U.S. government policy, but admitted they are meant to provide the Joint Forces with "an intellectual foundation upon which

we will construct the concept to guide out future, force developments." Source: http://www.guardian.co.uk/business/2010/apr/11/peak-oil-production-supply

U.S. attorney's office may investigate mine explosion in the future. A U.S. district attorney announced Monday that his office has not yet, but may sometime in the future launch an investigation into the Upper Big Branch Mine explosion that killed 29 and injured two others in Raleigh County, West Virginia. He said in a news release that his office normally doesn't confirm or deny whether it is involved in investigations. But he was compelled to do so in this case because of widespread public interest. "The United States Attorney's Office is ready, willing and able to receive any information and/or investigative reports regarding the explosion and subsequent deaths of the 29 miners at the Upper Big Branch Mine in Raleigh County, West Virginia." the attorney stated in the news release. "If the investigation undertaken by the Mine Safety and Health Administration reveals that criminal violations have occurred, we will work vigorously with investigators to pursue those offenses to the fullest extent of the law." Source: http://www.wboy.com/story.cfm?func=viewstory&storyid=78152&printview=1

Food and Agriculture

(Nebraska) **Neb. TB investigation draws nearer to close.** Despite the new case of bovine tuberculosis (TB) found in South Dakota in January that led to quarantine of four, northeast Nebraska herds, the Nebraska Department of Agriculture (NDA) director said the new case is "not indicative of a TB problem in Nebraska." In a public update on the TB issue, he offered details on the "wrap up" of the investigation into the June 2009 finding of two TB-positive beef cows in a Rock County herd. "We are extremely pleased that after extensive testing, we did not find any additional positive cases of TB in association with the Rock County investigation," the NBA director said. He said NDA staff, in coordination with federal animal disease officials, tested 21,764 head of cattle in association with the investigation of two TB-positive cows found in Rock County last year. A total of 61 herds in 20 counties were quarantined as NDA traced cattle movement into and out of the affected herd, and tested cattle that may have shared a fence line with the herd. No additional positive cases of TB were found. Ibach said only three herds remain under quarantine at this time, with those quarantines to be lifted as those feeder cattle move to slaughter. But the threat bovine TB poses to area cattlemen is not over yet. "Unfortunately, the disease has been found in association with another investigation," the NDA director said. NDA began working with South Dakota officials in January after they announced the finding of a TB-positive cow in the southeastern part of the state. Preliminary work to trace cattle movements into and out of the South Dakota herd included a link to Nebraska. General information about bovine TB can be found on the NDA Web site at www.agr.ne.gov. Source: http://www.yankton.net/articles/2010/04/15/community/doc4bc698075e5b6325342788.txt

Groups urge plan reversal for Brazilian beef. On Monday, 32 groups filed a joint letter to the U.S. Department of Agriculture (USDA) and the U.S. Trade Representative (USTR) urging both agencies to abandon plans to relax U.S. foot-and-mouth disease restrictions with regards to Brazilian beef and other livestock products. The letter came as a response to the joint news release issued by the agencies on April 6, announcing the proposed rule would be published in the April 16 Federal Register. The proposed rule would recognize the Brazilian state of Santa Catarina as free of foot-and-mouth disease, rinderpest, classical swine fever, African swine fever, and swine vesicular disease. The recognition would come based on World Organization for Animal Health guidelines. There is also a

current risk evaluation underway with aims to identify appropriate risk-mitigation measures to determine whether fresh beef can be imported from Brazil while preventing the introduction of foot-and-mouth disease into the United States. “United States consumers, farmers and ranchers deserve more protection against the risk of disease importation from their government, not less,” the groups wrote in an attempt to encourage the agencies to reconsider their actions. According to the USDA, foot-and-mouth disease is a severe, highly contagious viral disease of cattle and swine. It is not a threat to people and no human health risks are associated with the disease, but it also affects sheep, goats, deer, and other ruminants with cloven hooves. Foot-and-mouth disease is caused by a virus and signs of the illness in animals can appear after an incubation period of 1 to 8 days, but often develop within 3 days. There are seven known types and more than 60 subtypes of the foot-and-mouth disease virus. Source: http://www.foodsafetynews.com/2010/04/groups-urge-plan-reversal-for-brazilian-beef-due-to-foot-and-mouth/

ARS researching Camelina as a new biofuel crop. Agricultural Research Service (ARS) scientists have long-term studies underway to examine growing camelina as a bioenergy crop for producing jet fuel for the military and the aviation industry. This research supports the recently signed memorandum of understanding between the U.S. Department of Agriculture (USDA) and the Department of the Navy (DoN) and interests of the Commercial Airlines Alternative Fuels Initiative (CAAFI). Native to Europe, camelina (Camelina sativa) is a member of the plant family Brassicaceae and has been grown since ancient times for use as lamp fuel, among other things. The seed’s high oil content has made it a promising candidate as a new source for biofuels. Since 2006, ARS researchers and university collaborators throughout the country have been examining how to incorporate camelina and other oil seed crops into existing crop production systems. Preliminary results from Sidney, Mont., suggest that current camelina varieties use about as much water as spring wheat, so growers would still need to leave land fallow in alternate years to build up water or accept possible yield losses for wheat grown in rotation. However, with appropriate breeding and selection for uniform, desirable agronomic and oil-quality characteristics, camelina has potential to be a good oil seed crop for planting during fallow years. Also, scientists in Maricopa, Ariz., have identified a few lines of germplasm from the ARS camelina collection that are suitable for rotations with cotton. ARS camelina germplasm research concentrates on identifying high-yielding lines that industry can use to develop new cultivars suitable for different growing conditions across the country. Source: http://www.ars.usda.gov/is/pr/2010/100413.htm

Contaminant limits needed for U.S. beef. Americans are eating beef that contains pesticides, animal antibiotics and heavy metals, an audit prepared by a U.S. inspector general indicated. The Office of Inspector General for the U.S. Agriculture Department said the problem stems from the fact that responsible agencies haven’t set limits for contaminants and don’t adequately test for them, USA Today reports. Food safety inspectors can’t stop the distribution of beef with contaminants because the Environmental Protection Agency and the Food and Drug Administration haven’t established limits, the audit found. As an example, the audit report said that in 2008, Mexican authorities rejected a U.S. beef shipment because its copper levels exceeded Mexican standards. Because there was no U.S. limit established, food safety inspectors couldn’t prevent the rejected meat from being sold in the United States. The U.S. Food Safety and Inspection Service said it will work with the EPA and FDA on “corrective actions.” Source: http://www.upi.com/Health_News/2010/04/13/Contaminant-limits-needed-for-US-beef/UPI-12241271168689/

(California) **Tainted beef probed in California.** Government agencies are investigating the source of potentially contaminated ground beef sold at the WinCo Foods store in Modesto, California. WinCo issued a voluntary recall of all ground-beef products sold at the store from April 3 through Friday, after a food-testing laboratory advised WinCo on Friday that two samples of hamburger purchased from the store were tainted with E. coli bacteria. Stanislaus County health officials said Monday that they were not aware of anyone becoming sick from eating meat purchased from the WinCo store. Infection with E. coli often causes abdominal cramps and diarrhea, sometimes with bloody stool. The symptoms usually go away in five to 10 days, but the infection can lead to kidney damage or even death in a small percentage of cases. The contamination was in a single beef product that originates from a meat-processing facility outside California, according to a statement from the chief of the food, drug and radiation safety division of the California Department of Public Health. The state agency did not identify the meat supplier. State health officials are jointly investigating the contamination with the Stanislaus County Department of Environmental Resources and the U.S. Department of Agriculture. Source: http://www.azcentral.com/news/articles/2010/04/13/20100413calif-meat0413.html

Government Sector (including Schools and Universities)

(Florida) **Four schools receive bomb threats.** Four schools received e-mailed bomb threats on Wednesday afternoon, according to a representative of the School Board of Miami-Dade County. The spokesman said the e-mail threats were sent at about 1:30 p.m. The note said that a bomb would go off at 2 p.m., but nothing happened, officials said. The schools that received threats included Felix Varela Senior High School, Christina M. Eve Elementary School, Sunset Senior High School and Hialeah Miami Lakes Senior High School. The spokesman said that none of the schools were evacuated. The chief of the school police said threats are common, and that investigators have made progress in tracking down the person who sent the threatening e-mails. Source: http://www.justnews.com/education/23152837/detail.html

(Pennsylvania) **Arson fire damages National Guard Armory near Phoenixville.** Fire officials are investigating an arson fire that occurred early Thursday morning at the Pennsylvania Army National Guard Armory on Rapps Dam Road. Firefighters from Phoenixville, Kimberton, Valley Forge, Liberty Fire, Ridge and Lionville responded to the blaze around 4:30 a.m. Once firefighters got the blaze under control, fire officials began their investigation. They determined that a person or persons broke into the armory building and started the fire while inside, according to state police at Embreeville. Nothing was taken from the building, and all weapons stored inside the armory are accounted for and have been secured, police said. The fire resulted in "significant structural damage," according to state police. State police and Chester County fire marshals are continuing to investigate. The armory is the headquarters of the 56th Stryker Brigade, 111th Infantry. Source: http://www.pottstownmercury.com/articles/2010/04/15/news/doc4bc7270180f6b864366452.txt

Secretary Napolitano announces enhancements to protect federal facilities. The DHS Secretary Monday announced two enhancements to federal facility security — initiatives that further strengthen the department's ability to protect thousands of government buildings across the United States one week prior to the anniversary of the Oklahoma City bombing. The DHS-led Interagency

Security Committee (ISC) released new standards establishing baseline physical security measures for all federal buildings and facilities — bolstering protection against terrorist attacks and other threats based on ongoing risk assessments. The standards announced include the Physical Security Criteria for Federal Facilities, which establishes comprehensive standards to address site, structural, interior and system security, as well as security operations and administration; and the Design-Basis Threat Report, designed to inform these customizable standards with current threat-based intelligence. The new standards will undergo a 24-month validation period of field testing and implementation by the federal security community. The ISC will publish final editions of the standards following this period. In addition, DHS' Federal Protective Service Monday announced the next deployment phase for the new Risk Assessment and Management Program (RAMP) — a computer-based tool that enhances access for FPS Inspectors to information about security threats and risks associated with more than 9,000 facilities owned and leased by the General Services Administration. Source: http://www.dhs.gov/ynews/releases/pr_1271098574316.shtm

Feds: Synagogue bomb suspect wanted to shoot President. The lead terror suspect in last year's alleged plot to bomb synagogues in the Bronx (New York) claimed he wanted to shoot the former President "700 times" and repeatedly called the leader of Al Qaeda "my brother," according to transcripts of FBI recordings filed in federal court Tuesday. The suspect was charged last May with recruiting three others to try to carry out attacks on Jewish temples in the Riverdale section of the Bronx as well as plotting to shoot down airplanes at Stewart Air base in Newburgh, N.Y. The four men have pleaded not guilty and defense lawyers have claimed the group was set up by an FBI informant. Source: http://www.nbcnewyork.com/news/local-beat/Feds-Synagogue-Bomb-Suspect-Wanted-To-Shoot-President-700-Times-90770714.html

Guns, knives, fake bombs allowed into federal buildings, tests show. Federal Protective Service contract guards failed to detect guns, knives and other prohibited items brought into federal agencies more than half of the time during covert tests conducted last year by the agency, the Government Accountability Office reviewed in a new report. In addition, many FPS contractor guards stationed at federal buildings continue to lack proper training and certification requirements, a problem cited last year in a previous GAO report. The agency still has not taken disciplinary actions against companies who employ those guards for noncompliance. In fact, the agency extended contracts for the seven companies surveyed by GAO, even though none of them was in compliance with training and certification requirements, GAO said in its new report, obtained by Federal Times. The chairman of the Senate Homeland Security and Governmental Affairs Committee said the new report shows FPS continues to face widespread problems with its contractor workforce. "While it has taken some steps forward in recent months, the Federal Protective Service continues to be an agency in crisis," he said. The newest GAO report follows on a series of eye-opening reports GAO issued in the past year detailing security lapses and other shortcomings by the contract guards. In July, for instance, GAO reported that its undercover investigators were able to smuggle bomb-making components into 10 high-security federal buildings. Since that July report, FPS has conducted 53 covert tests in the same regions that the GAO visited. The guards identified guns, knives and fake bombs in 18 tests, but failed to identify the items in 35 tests, GAO said in the new report. Source: http://www.federaltimes.com/article/20100413/FACILITIES02/4130306/1001

GAO: Federal computers still not defended against cyber threats. Federal agencies remain vulnerable to cyber attacks and security breaches because they've failed to take required steps to

secure Internet connections and computer systems, the Government Accountability Office said in two reports issued today. No agency has taken all of the actions required to secure their Web networks under the Trusted Internet Connections and Einstein programs, GAO said in the report, "Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies." GAO largely faulted the Office of Management and Budget and the Homeland Security Department for the delays, saying they provided "inconsistent communication" to agencies for how to secure their Web connections. GAO also reviewed efforts to roll out the Federal Desktop Core Configuration initiative, which was launched by OMB and the National Institute of Standards and Technology in 2007 and is supposed to provide a baseline level of security for government-owned desktop and laptop computers. No agency has deployed all of the configuration settings on all of their workstations as required under the initiative, GAO said in the report, "Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements." Source: http://www.federaltimes.com/article/20100412/IT01/4120303/1001

(Georgia; Florida) **3 dead after Navy plane crashes in Georgia.** A Florida-based Navy plane just missed a house and crashed in dense woods in north Georgia on Monday, killing three crew members, and authorities were looking for a fourth person believed to be aboard, officials said. A Naval Air Station Pensacola spokesman said authorities have not confirmed whether the pilot was among those killed when a T-39N training plane went down at 4:26 p.m. No one on the ground was injured, he said. The plane was part of Training Air Wing 6, which conducts routine cross-country missions through Fannin County, where it crashed, about two hours north of Atlanta, on the edge of the North Carolina and Tennessee borders, he said. Searchers found three bodies. The twin-jet plane can carry two pilots and seven passengers, according to a Navy Web site. Authorities do not know what caused the plane to go down and are putting together an investigative team, he said. He did not release the victims' names and said he didn't know where the plane had originated. A Federal Aviation Administration spokeswoman said the agency is not investigating the military crash. Source: http://www.foxnews.com/us/2010/04/12/dead-naval-aircraft-crashes-georgia/?test=latestnews

Senate peppers Pentagon with questions on electronic warfare, stalling cyber command launch. The nomination of a lieutenant general to head the Pentagon's Cyber Command has given senators leverage to delve into the complex world of cyber warfare. Later this week, the lieutenant general nominated to lead the new agency will be grilled at a Senate committee hearing. The Cyber Command would oversee military networks and take on what U.S. authorities see as a growing national security threat — cyber terrorists looking to steal sensitive technologies, disrupt critical services, or infiltrate classified networks. The hearing will likely touch on issues such as how the U.S. should fight back when hackers a continent away attack a military computer system, using computers belonging to unsuspecting private citizens or businesses as cover. Taking action against a hacker could affect foreign countries, private citizens or businesses — ranging from hospitals to power plants — whose computers might get caught up in the electronic battle. Difficult questions about how and when the U.S. military conducts electronic warfare have stalled the creation of the Cyber Command for months. Source: http://www.latimes.com/news/nationworld/politics/wire/sns-ap-us-waging-cyber-war,0,303953.story

(Maryland) **Hazmat crews investigate suspicious package.** Baltimore County fire and hazmat crews responded Saturday to a report of a suspicious package at the U.S. Census Data Capture Center. It happened about 11 a.m. in the 8400 block of Kelso Drive in Rosedale. Baltimore County police said

four people complained of some undisclosed medical problems after coming into contact with a white powdery substance at the Data Capture Center, although they refused medical treatment. The substance was determined not to be a threat. Police would not say if the incident was related to previous hazmat calls at the Data Capture Center, which were being investigated by Baltimore County police. The FBI was not involved in the investigation. Source: http://www.wbaltv.com/news/23112217/detail.html

Bomb damages U.S. consulate in Nuevo Laredo. A bomb damaged the outside of the U.S. Consulate in the border city of Nuevo Laredo, Mexico overnight, but there are no injuries, the U.S. Embassy in Mexico City said. An embassy spokesman said the explosive device was thrown over the wall of the consulate across the border from Laredo at around 11 p.m. Saturday. According to a posting on the consulate's Web site, the explosion damaged windows. The Consulate General and Consular Agency in Piedras Negras will be closed Monday, the posting said. "The Consulate General and Consular Agency will reopen when we are confident that we have adequate security to keep our visitors safe," the posting said. Source: http://www.kwtx.com/nationalnews/headlines/90568319.html

Information Technology and Telecommunications

Senator pledges support for Net neutrality, broadband plan. The powerful chairman of a U.S. Senate committee will push for additional authority for the U.S. Federal Communications Commission (FCC) to enforce Net neutrality rules and implement its new national broadband plan, if it is needed following a court ruling against the agency this month. The decision by the U.S. Court of Appeals for the District of Columbia to throw out the FCC's attempt to enforce Net neutrality rules against Comcast puts the entire broadband plan, released last month, at risk, said a West Virginia Democratic senator and chairman of the Senate Commerce, Science and Transportation Committee. Comcast and other broadband providers want to take the FCC's authority away, the senator added. "In the long term, if there is a need to rewrite the law to provide consumers and the FCC and industry with a new framework, I as chairman will take that task on," he said. "This is a committee — at least so long as I am chairman — that is here to protect people, to protect consumers." Source: http://www.computerworld.com/s/article/9175507/Senator_pledges_support_for_Net_neutrality_broadband_plan

Chinese cyber attackers hit Optus. The Optus network was in disarray April 14, following cyber attacks from China, which affected a number of its customers including Australia's national news agency, AAP. Web-based attacks originating from China have become a growing issue for Australian businesses and government departments. At the opening of the Cyber Security Operations Centre in January, the government revealed that Defence had investigated about 200 electronic-security incidents on its own network every month in 2009. It also responded to about 220 incidents reported by other Australian government agencies last year. Optus indicated that at about 1:10 p.m. April 14, one of its corporate customers was hit with a "denial of service attack" that originated in China. Optus would not say which customer had been targeted, but The Australian reported that the target was a multinational, financial-services company. "The attack caused congestion on one of Optus's international links leading to slow internet and delayed e-mail for some Optus corporate customers," an Optus spokeswoman said. Publishers AAP, IDG and News Ltd are known to be among the affected corporate customers. Source: http://www.smh.com.au/technology/security/chinese-cyber-attackers-hit-optus-20100415-sgm8.html

DNS Trojan poses as iPhone unlocking utility. An application that offers to unlock iPhones is actually designed to hijack Internet connections on compromised Windows PCs, security watchers warn. Spam messages direct potential victims to a domain called iphone-iphone.info that offers links to download a Windows-executable called blackra1n.exe. The application claims to offer an unlock utility but instead it changes default DNS settings on infected Windows PCs, hijacking Internet connections in the process. Romanian anti-virus firm BitDefender, which identifies the executable as Trojan-BAT-AACL, explains that the malware comes as a Windows batch file packed alongside the iPhone jailbreaking application. "The Trojan attempts to change the preferred DNS server address for several possible Internet connections on the users' computers to 188.210.[REMOVED]," BitDefender explained. "This allows the malware creators to intercept the victims' calls to reach Internet sites and to redirect them to their own malware-laden versions of those sites." Source: http://www.theregister.co.uk/2010/04/15/iphone_unlocking_trojan_scam/

Next-Generation clickjacking attacks revealed. A researcher at Black Hat Europe will demonstrate a new, powerful breed of clickjacking attacks he devised that can bypass newly constructed defenses in browsers and Websites. The security consultant with Context Information Security in the U.K., also will release a browser-based point-and-shoot tool for clickjacking that simplifies these attacks on Web applications and provides researchers visual views of the links, buttons, fields, and data to be targeted by the clickjacking attack. Clickjacking occurs an attacker slips a malicious link invisibly on a Web page or under a button on the site. When the user clicks on the link or moves his mouse over it, he becomes infected. Facebook and Twitter both have suffered from clickjacking. To date, clickjacking alone has been considered a fairly, limited attack except when it is paired with cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. Source: http://www.darkreading.com/vulnerability_management/security/app-security/showArticle.jhtml?articleID=224400129

FBI warns about online census scams. The Internet Crime Complaint Center on April 12 warned Americans to be careful about potential Web and other scams related to the 2010 census. The center, a joint venture between the FBI and the National White Collar Crime Center, warned that census takers will not contact U.S. residents seeking census information via e-mail or seek donations. It also notes that census takers will not ask for personally identifiable information such as Social Security Number and bank account number. It advised computer users to not respond to e-mail or other solicitations. "Criminals often capitalize on legitimate campaigns to spread computer viruses through e-mails, text messages, 'pop-ups,' fraudulent Web sites, or infected legitimate Web sites," according to an alert from the center. It added that viruses can be embedded in e-mail attachments, links, or even pictures and that anti-virus software may not detect all viruses especially those that are newly created. The center said U.S. residents should be wary of similar tactics being used on social networking sites as well. The alert also warned users to watch out for e-mail and other scams offering potential jobs with the Census Bureau. "The Census Bureau has a hiring process, which includes taking a test in person, not online," the center added. Source: http://www.nextgov.com/nextgov/ng_20100412_5056.php?oref=topnews

Nearly 90 percent of firms show Zeus botnet activity. Most major U.S. corporations — up to 88 percent of the Fortune 500 companies — may be affected by botnet activity from computers compromised by the Zeus, data-stealing, Trojan virus, according to an RSA study released on April 14.

RSA's FraudAction Anti-Trojan services analyzed data stolen by Zeus from infected computers in August and traced evidence back to IP addresses and e-mail addresses belonging to the corporations, said the manager of the Identity Protection and Verification Group at RSA, which is the security division of EMC. Among the stolen data found on the sites where infected computers drop the stolen data was compromised e-mail addresses from about 60 percent of the firms. Companies with fewer than 75,000 employees appeared to have the highest ratio of botnet activity and compromised e-mail addresses to employee counts, according to the report. Source: http://news.cnet.com/8301-27080_3-20002425-245.html

Microsoft, Adobe, Oracle unite with massive patch batch. It was an extreme version of Patch Tuesday as Microsoft, Adobe Systems, and Oracle released updates that fixed dozens of critical vulnerabilities in their wares. As part of Microsoft's monthly patch regimen, the software giant issued 11 updates that patched a total of 25 bugs. At least eight of the vulnerabilities are likely to be targeted by reliable exploits in the wild, Microsoft officials said. Adobe, meanwhile, fixed 15 security flaws in its Reader and Acrobat software for viewing PDF files. The software maker rated the update "critical," meaning attackers can exploit the bugs to take control of end-users' computers. Oracle released 47 updates of its own to patch security bugs in a variety of applications, including Database Server, Fusion Middleware, Collaboration Suite, E-Business Suite, and PeopleSoft Enterprise. Source: http://www.theregister.co.uk/2010/04/13/extreme_patch_tuesday/

Microsoft tries to avoid windows blue screen repeat. Microsoft took steps on April 13 to avoid repeating the debacle two months ago that left Windows XP users staring at the notorious "Blue Screen of Death" error message after they applied a patch. In February, a security update that fixed two flaws in the Windows kernel — the operating system's most important component — wreaked havoc when it was applied by users, who almost immediately flooded Microsoft's support forum with reports of crippled computers . As the number of reports grew, Microsoft first stopped automatically serving the MS10-015 update, then confirmed that a rootkit caused the crashes. Only PCs that had been previously infected with the Alureon rootkit were incapacitated, Microsoft's investigation found. MS10-021, one of the 11 updates issued on April 13 as part of Microsoft's monthly Patch Tuesday cycle, also fixed flaws in the Windows kernel. But Microsoft is hoping that this month's update will not trigger a repeat Blue Screen of Death episode. Source: http://www.pcworld.com/article/194205/microsoft_tries_to_avoid_windows_blue_screen_repeat.html

Third of XP security suites flunk tests. A third of 60 anti-malware products for Windows XP failed to make the grade in independent security tests. Twenty out of 60 security products tested by independent security-certification body Virus Bulletin flunked its rigourous VB100 certification, mainly because of false-positive problems. False alarms in scanning benign files from major providers including Adobe, Microsoft, Google and Sun tripped up many of the products under test. Failure to detect complex polymorphic viruses also acted as a stumbling block during Virus Bulletin's largest ever test of anti-malware products to date. Win XP security products from Microsoft, Frisk, Norman and Fortinet were among those who failed to make the grade. Source: http://www.theregister.co.uk/2010/04/13/winxp_anti_malware_tests/

Microsoft to patch unhackable Windows 7 bug later today. On April 13, Microsoft will play it safe by patching a Windows 7 bug that it says cannot be exploited. Of the 11 security bulletins that will be

released in a few hours, Bulletin 7 will address one or more vulnerabilities in Windows 2000, Windows XP and Windows Server 2003. But Microsoft will also offer the same update to users running Windows Vista, Windows 7 and Windows Server 2008, even though the company maintained last week that they were impervious to attack. "Windows 7 users will be offered Bulletin 7 as a defense-in-depth update even though the [advanced notification] states that the issue does not affect Windows 7," said a group manager with the Microsoft Security Response Center, in one of several e-mails replying to questions. "This means that the vulnerable code is in the software, but due to the improved protections built into Windows 7, there are no known vectors to reach it." In other words, the vulnerability is there — in Vista, Windows 7 and Server 2008 — but Microsoft doesn't know how it could be exploited. Source: http://www.computerworld.com/s/article/9175402/Microsoft_to_patch_unhackable_Windows_7_bug_later_today

Researcher warns of impending PDF attack wave. A design flaw in Adobe's popular PDF format will quickly be exploited by hackers to install financial malware on users' computers, the CEO of security company Trusteer argued April 9. The bug, which is not strictly a security vulnerability but actually part of the PDF specification, was first disclosed by a Belgium researcher the week of March 29. He demonstrated how a multistage attack using the PDF specification's "/Launch" function could successfully exploit a fully-patched copy of Adobe Reader. Adobe has acknowledged the bug, but has not yet committed to producing a patch to stymie attacks. However, the company has urged users to change Reader's and Acrobat's settings to disable the /Launch function. In a blog post April 6, the Adobe Reader group product manager recommended that consumers block attacks by unchecking a box marked "Allow opening of non-PDF file attachments with external applications" in the programs' preferences panes. By default, Reader and Acrobat have the box checked, meaning that the behavior the researcher exploited is allowed. The product manager also showed how enterprise IT administrators can force users' copies of Reader and Acrobat into the unchecked state by pushing a change to Windows' registry. On April 8, another Adobe executive said Adobe is considering several options to plug the hole, among them an update to Reader and Acrobat that would change the default state of the setting to off. Source: http://www.computerworld.com/s/article/9175159/Researcher_warns_of_impending_PDF_attack_wave?taxonomyId=17&pageNumber=1

Facebook 'Farm Town' users hit by malicious ad linked to fake antivirus. Users of the popular Facebook game "Farm Town" were hit with a rogue antivirus scam tied to malicious advertising. SlashKey, the developer behind "Farm Town," issued a warning about the malware scam, which drew hundreds of comments to its user forum. According to findings by a researcher, the ad in question was a banner advertisement for greeting cards. If it is displayed, the user is redirected to various sites and eventually lands on one pushing rogue antivirus. "If you suddenly get a warning that your computer is infected with viruses and you MUST run this scan now, DO NOT CLICK ON THE LINK, CLOSE THE WINDOW IMMEDIATELY," SlashKey warned in a post to its user forum. "You should then run a full scan with your antivirus program to ensure that any stray parts of this malware are caught and quarantined." Reports of users getting infected continued to come through early Monday morning; however, the researcher has since posted in the user forum that the ad network serving the malicious ad has identified and disabled it. Source: http://www.eweek.com/c/a/Security/Facebook-Farm-Town-Users-Hit-by-Malicious-Ad-Linked-to-Fake-Antivirus-550801/

National Monuments and Icons

(Utah) **3.9 magnitude earthquake rocks Capitol Reef National Park.** The University of Utah Seismograph Stations reports that a minor earthquake of magnitude 3.9 occurred in Capitol Reef National Park in southern Utah, at 12:58 PM on April 14, 2010 (MDT). The epicenter of the shock was located 26 mi SE of Torrey, Utah and 31 mi NE of Escalante, Utah. A total of 8 earthquakes of magnitude 3.0 or greater have occurred within 16 mi of the epicenter of this event since 1962. Source: http://www.kcsg.com/view/full_story/7079433/article-3-9-Magnitude-Earthquake-Rocks-Capitol-Reef-National-Park-?instance=home_stories1

(Pennsylvania) **Deal made on paying for cleanup of Valley Forge park.** A hiker and her husband were looking for a path through the woods at Valley Forge Park when they saw the danger signs tacked up on a fence. "Asbestos, cancer and lung-disease hazard," the sign read. "Respirators and protective clothing are required." The hiker, a nurse, tried not to breathe too hard as she backed away. This week, the National Park Service announced a plan with the state to pay for a cleanup of the contaminated 112-acre site - 13 years after workers discovered asbestos while burying fiber-optic cable there. Under the consent decree, expected to go into effect after a public comment period, the state would foot 60 percent of the estimated $12 million cleanup, and the federal government would pay the rest. To clean it up about three feet of the topsoil in the woods and meadows will be scraped off and new dirt brought in to replace it. The area is to be reopened to visitors within two years. The contamination dates back to the late 19th and mid-20th centuries, when an asbestos-insulation plant operated in what is now the park. From about 1925 until the 1970s, the plant and its predecessor dumped their waste into limestone quarries there and onto property owned by the state - with the state's permission, according to the park service. Source: http://www.philly.com/philly/news/local/90451244.html

(Montana) **Climate change threatening Glacier National Park and Montana's economy.** Climate change is seen as threatening the ecology of Glacier National Park in a new report from the Rocky Mountain Climate Organization and the Natural Resources Defense Council. A just-completed update by the U.S. Geological Survey finds that of the 37 named glaciers in the park, only 25 remain large enough to still be considered glaciers. Glacier is on track to lose all or nearly all of its glaciers, Seven years ago, scientists projected that even modestly hotter summers could eliminate all glaciers in one basin in the park by 2030. Since that study was published, the glaciers in the basin have melted faster than projected. One author of that study, from the U.S. Geological Survey's Northern Mountain Science Center, says the basin's glaciers could be gone in just 10 years. Tourism is Montana's number 2 industry which brings in almost $3 billion to the state's economy, and Glacier National Park is a "top draw." The loss of the glaciers and their dependent ecosystems would no doubt lessen the appeal of the park and result in a large monetary loss to the Montana economy. Source: http://www.examiner.com/x-8180-Portland-Green-Business-Examiner~y2010m4d9-Climate-change-threatening-Glacier-National-Park-and--Montanas-economy

Postal and Shipping

(Arizona) **FD: Powder found in package mailed to US Attorney's office.** Crews responded to a downtown Phoenix building after an unknown powder was discovered in a package at the U.S.

Attorney's office on Monday morning. Fire officials said a small package was delivered and was placed through the X-ray machine on the twelfth floor of a building near Central and Washington. A spokesperson for the Phoenix Fire Department said a powder was seen inside the package, but the package was never opened so no one was exposed to it. He said the package was removed from the building for officials to examine it. There were no evacuations and no injuries. Source: http://www.abc15.com/content/news/phoenixmetro/central/story/FD-Powder-found-in-package-mailed-to-US-Attorney/R6K7YNgokUOpbu3zgPsxJA.cspx

(Iowa) **Officials probe five mailbox bombings in Clive, W.D.M.** Two bombs set off at two residences in West Des Moines, Iowa and three in Clive, Iowa that occurred last week have the same explosive components, a police sergeant said. The week of April 5-9 saw the latest incident of a homemade bomb destroying a mailbox in the western suburbs. Three mailboxes in Clive and two in West Des Moines have been destroyed in recent weeks. No one has been hurt. Police officers and postal inspectors are investigating the incidents. A West Des Moines police lieutenant said investigators are taking the incidents very seriously. "We don't want anybody's property to be damaged, and we don't want anybody to be hurt," the lieutenant said. The bombs, made from plastic bottles and household chemicals, are fairly easy to make, but can be dangerous because of their unpredictability. The time it takes for them to explode can vary by several minutes. A Clive police sergeant said they can not say for sure what might have triggered the rash of incidents, but the bombs have all had the same components. "Our thought is it's probably the same group of people," the sergeant said. Source: http://www.desmoinesregister.com/article/20100413/NEWS/4130306/1001/NEWS/Officials-probe-five-mailbox-bombings-in-Clive-W.D.M

(Montana) **Envelope with suspicious white powder found at Federal Reserve Bank.** Authorities are investigating a suspicious white powdery substance workers found Monday afternoon leaking out of an envelope that had been sent to the Federal Reserve Bank on Neill Avenue in Helena, Montana. Police were called to the scene about 1:20 p.m., according to an assistant chief. Several employees who handled the envelope were moved to a different part of the building, but the building was not evacuated. A hazardous-materials team with the Helena Fire Department was dispatched to the scene. A Helena Police Department spokesman said the powder is being tested at the state health department lab. "Due to the suspicious nature of the envelope, it was seen as a threat," the police spokesman said. The president of the Federal Reserve Bank branch said an initial analysis showed no hazardous material. "They're doing some further analysis, and safety is of course paramount to us," he said. The branch president said the envelope was not opened by bank employees. Investigators declined to say whether the envelope had a return address, what kind of envelope it was or whether it contained anything other than the powder. Source: http://billingsgazette.com/news/state-and-regional/montana/article_109b7a90-4695-11df-b1b4-001cc4c002e0.html

(Massachusetts) **Boston Police Department powder mail threat probed.** Envelopes holding what officials feared was a toxic brown powder — but proved to be ground tea leaves — arrived in the mail April 9 at five Boston police precinct stations, causing one to be evacuated as a hazmat team examined the package, authorities said. A Boston Police Department spokeswoman said detectives identified a suspect, but she could not say how they traced the envelopes to the man, whose identity was shared with U.S. Postal Inspectors leading the probe. Police declined to release his name or say whether the envelopes contained letters, but a law enforcement source said, "He's in a hospital in Massachusetts being treated for mental illness." Source:

http://news.bostonherald.com/news/regional/view/20100410boston_police_department_powder_mail_threat_probed_substance_idd_as_tea_leaves/

Public Health

Hospital infection problem persists. The nagging and largely solvable problem of hospital-acquired infections remains as resistant to cure as the germs that contribute to an estimated 100,000 deaths a year, according to an annual government study issued Tuesday. Despite a renewed focus on prevention and threats of governmental sanctions, hospitals continue to see increased rates of post-operative, bloodstream infections and catheter-associated urinary tract infections, the Agency for Healthcare Research and Quality reported. The rates increased by 8 percent for bloodstream infections and 4 percent for urinary tract infections over the previous year. There was no change in the incidence of bloodstream infections caused by the placement of catheters in central veins. The only positive news came from a 12-percent reduction in the rate of post-operative pneumonia.The report concluded that hospital-acquired infections merited "urgent attention." Source: http://www.nytimes.com/2010/04/14/us/14infect.html

(Tennessee) **Medical records secured by code-changing algorithm.** Researchers at Vanderbilt University in Tennessee have come up with a new method to categorize medical data to protect identity wihout interfering with the medical and genetic inter-data connections needed for research, Scientific American reported. The algorithm the researchers developed, exchanges publicly known patient ICD codes with another code system. This could help researchers who have long looked to medical-records databases to map trends in diseases and study them to discover better treatment methods. But the problem has been that the detailed patient data with codes for every disease, symptom or injury are available through public databases and electronic medical records, where the anonymized data can be tied to individuals. To prove that this is a realistic problem, the Vanderbilt research team conducted an experiment which resulted in 96 percent of the 2,762 patients belonging to the test group identified through diagnosis codes. The researchers tested the algorithm they developed it by simulating a hacker attack, with the premise that the hacker is privy to the patients' identity, their ICD codes and the fact that the patients' data is included in the database. The test was completely successful: the hacker could not uncover the patient's private information, and the information remained useful for research. Source: http://www.net-security.org/secworld.php?id=9128

Transportation

(Colorado) **FBI investigating lasers being aimed at aircraft.** The FBI is investigating two cases where laser lights were aimed at aircraft flying over Denver. One of the cases was reported late on the evening of April 8 near Castle Rock, Colorado. It is not clear if the aircraft were commercial or private. Source: http://www.thedenverchannel.com/news/23109011/detail.html

(New York) **Details emerge in Al Qaeda plot on NYC subway system.** A fourth suspect in the alleged plot to blow up New York City subways has reportedly revealed more details about the plan. The Queens native and two high school friends were planning to detonate explosives attached to their bodies at Grand Central and Times Square stations during rush hour, according to the NY Daily News.

The paper reports that the fourth suspect was arrested in Pakistan and is likely to be extradited to Brooklyn. The group had supposedly picked September 14, 15, or 16 as the attack date. The would-be bomber said in court that he gave up on his terror plot after he learned the FBI and NYPD were aware of his plan. Source: http://www.foxnews.com/us/2010/04/12/details-emerge-al-qaeda-plot-nyc-subway/

Water and Dams

Security incidents rise in industrial control systems. While only about 10 percent of industrial-control systems are actually connected to the Internet, these systems that run water, wastewater, and utility power plants have suffered an increase in cybersecurity incidents over the past five years. A new report based on data gathered by the Repository of Industrial Security Incidents (RISI) database provides a rare look at trends in malware infections, hacks, and insider attacks within these traditionally cloistered operations. Cybersecurity incidents in petroleum and petrochemical control systems have declined significantly over the past five years — down more than 80 percent — but water and wastewater have increased 300 percent, and power/utilities by 30 percent, according to the 2009 Annual Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems. The database logs security incidents in process control, Supervisory Control And Data Acquisition (SCADA), and manufacturing systems, and gathers voluntary submissions from companies as well as from news or other reports. Nearly half of all security incidents were due to malware infections — viruses, worms, and Trojans, according to the report. With only a fraction of control systems connected to the Internet, these infections are occurring in other ways: "A lot of control systems are connected to their business networks which in turn may be connected to the Internet. It's several layers removed, but once there's a virus [on the business network], it finds its way into the control systems," said the executive director of the Security Incidents Organization, which runs the RISI database. "And you see USB keys bringing in malware" to the SCADA systems, for instance, or via an employee's infected laptop, he said. Source: http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=224400280

The consequences of ignoring water risks in the US. Failure to address water risks and other critical issues posed by aging or inadequate infrastructure could further impede the U.S. economy and America's attempts to regain global competitiveness on a number of fronts, a new study warns. That is the conclusion of Infrastructure 2010: Investment Imperative, the fourth in an annual series of reports produced by the Urban Land Institute and Ernst & Young that examine infrastructure trends around the globe. Earlier reports focused on transportation, and the latest report updates previous findings with information showing that the U.S. continues to lag behind Asia and Europe in investments in transit systems. In addition this year, the report takes its first hard look at water issues. "Falling behind global competitors, the United States struggles to gain traction in planning and building the critical infrastructure investments that are necessary to ensure future, economic growth and support a rapidly expanding population," the report stated. "Perhaps no other infrastructure category presents the United States with greater challenges than water." One of the researchers said, "Bottom line, the U.S. is seriously threatening not only its quality of life now and for the future but also its very basic ability to compete economically with the rest of the world." Source: http://www.businessgreen.com/business-green/news/2261317/consequences-ignoring-water

(California) **Calexico water treatment plant damaged.** Calexico (Calif.) Water Plant operators say the plant is working at 50-percent capacity. City of Calexico residents are being urged to conserve water. The Calexico Water Plant facility manager said the main clarifier and the plant's three water tanks suffered major damage from the recent, 7.2 magnitude earthquake. He said the estimated repair cost is between $17 and $22 million. Source: http://www.kyma.com/slp.php?idN=3449

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295; email: ndslic@nd.gov ; FAX: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**